UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

TIFFANY PICKLESIMER, on behalf of herself and a class of similarly situated persons, Plaintiff, v. CONNECTONCALL.COM, LLC and PHREESIA, INC., Defendants.	**CASE NO.:** 2:25-cv-00324 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Tiffany Picklesimer, individually and on behalf of all others similarly situated ("Plaintiff"), brings this action against Defendants Phreesia, Inc. ("Phreesia"), a Delaware Corporation, and ConnectOnCall.com, LLC ("ConnectOnCall"), a wholly owned subsidiary of Phreesia (collectively "Defendants") seeking monetary damages, restitution, and/or injunctive relief for the proposed Class, as defined below. Plaintiff makes the following allegations upon information and belief, the investigation of their counsel, and personal knowledge or facts that are a matter of public record.

I. INTRODUCTION

1. The release, disclosure, and publication of sensitive, private data can be devasting. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have grave consequences for victims for years after the actual date of the breach—with the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans,

[1] Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, 25 S.C. LAWYER 28-35 (May 2014), https:// https://articlegateway.com. (last accessed June 13, 2024).

obtain medical services, obtain government benefits, and/or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information. Moreover, the release, disclosure, and publication of private medical information, such as diagnosis, medications and prescriptions can lead to sophisticated and costly insurance fraud, as well as embarrassment, humiliation and blackmail.

2. Defendant Phreesia is a Software company that manages the patient intake process, appointment scheduling, payment collection, and patient communications for healthcare organizations.[2] Defendant ConnectOnCall is a wholly owned subsidiary of Phreesia. On its website, Defendant Phreesia advertises a service called PhreesiaOnCall, "a medical answering solution that helps you manage after-hours calls and simplify care coordination with smart, automated call tracking."[3] According to the Google Play App store, "PhreesiaOnCall (previously ConnectOnCall) is an innovative, digital, after-hours solution for physicians who take a call … designed to allow all important patient related calls to be handled reliably and securely; requiring essentially no learning curve to get started."[4]

3. On May 15, 2024, Phreesia disclosed on its website that "a cybercriminal had gained access to ConnectOnCall."[5] Defendants admitted that they were subject to a data breach that occurred between February 16, 2024, and May 12, 2024 (the "Data Breach") and claim they first discovered the breach on May 12, 2024.[6] In the three months that their system was compromised, approximately 914,138 patients were impacted.[7] Information exfiltrated in the breach includes patient names, phone numbers, dates of birth, medical record numbers, health

[2] *See* https://www.phreesia.com/ (last visited Jan. 6, 2025).

[3] *See* https://www.phreesia.com/after-hours/ (last visited Jan. 2, 2025).

[4] PhreesiaOnCall, https://play.google.com/store/apps/details?id=com.connectoncall.connectoncall&hl=en (last visited Jan. 2, 2025).

[5] ConnectOnCall Security Incident Update, https://www.phreesia.com/security-incident/ (last visited Jan. 2, 2025).

[6] *See*, ConnectOnCall Data Breach, https://optimhealthsystem.com/connectoncall-data-breach/ (last visited Jan. 2, 2025).

[7] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Jan. 6, 2025).

conditions, treatment information, prescription information, and some social security numbers.[8] This information constitutes personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiff and other individuals ("the Class").

4. On December 11, 2024, Defendants finally reported the Data Breach to the United States Department of Health and Human Services, Office for Civil Rights and began mailing individual notification letters.[9] Thus, Defendants waited more than six months after they detected the Data Breach to notify the public.

5. Defendants garner revenue of hundreds of millions of dollars each year. In 2023 alone, Phreesia boasted revenues of $356,299,000.[10] Defendants further demonstrate extraordinary year over year annualized growth as their revenue for the nine months ending October 31, 2024, was $360,617,000, exceeding their entire 2023 total.[11] Defendants easily could have allocated a small portion of their burgeoning revenues toward cybersecurity and prevention to forestall and prevent the Data breach. But Defendants chose profits over protection of patients' most sensitive PII and PHI.

6. As a result of the Data breach, through which their PII and PHI were compromised, disclosed, and obtained by unauthorized third parties, Plaintiff and Class members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft for a period of years, if not decades. Furthermore, Plaintiff and Class members must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. And they must make family and close friends aware that personal health information about class members could be used in fraud and phishing attempts targeting their friends and

[8] Steve Alder, *ConnectOnCall Announces 914K-Record Data Breach*, The HIPAA Journal, (December 16, 2024) https://www.hipaajournal.com/connectoncall-data-breach/ (last visited Jan. 2, 2025).

[9] *Id.*

[10] *Phreesia Announces Fourth Quarter Fiscal 2024 Results*, Phreesia, Dec. 5, 2023 https://ir.phreesia.com/news/news-details/2024/Phreesia-Announces-Fourth-Quarter-Fiscal-2024-Results/default.aspx (last visited January 2, 2025).

[11] *Id.*

families. Consequently, Plaintiff and the other Class members will incur ongoing out-of-pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft and other fraudulent behavior.

7. By this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose private information was accessed during the Data Breach.

II. JURISDICTION, VENUE, AND CHOICE OF LAW

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

9. This Court has personal jurisdiction over Defendant ConnectOnCall because its principal place of business is located in the State of New York, it has sufficient minimum contacts with this district, and it has purposefully availed itself to the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

10. This Court has personal jurisdiction over Defendant Phreesia because it has sufficient minimum contacts with this district and it has purposefully availed itself to the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Defendant ConnectOnCall resides in this district, Defendants conduct substantial business within this District, and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. PARTIES

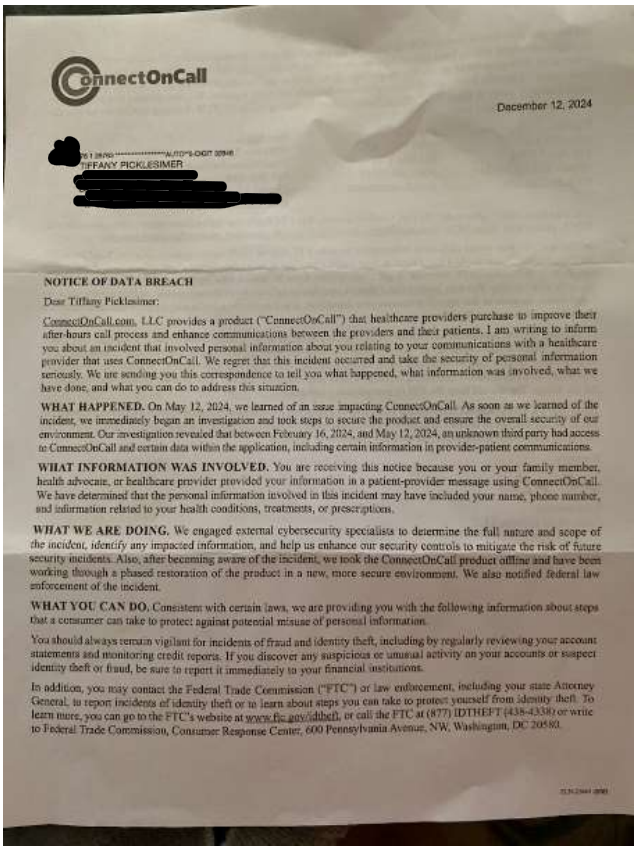
A. Plaintiff

12. Plaintiff Tiffany Picklesimer is a citizen of and is domiciled in the State of Florida.

13. Plaintiff provided confidential and sensitive PII and PHI to Defendants in connection with Defendants' provision of their services. Defendants obtained and continue to maintain Plaintiff's PII and PHI and have a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

14. Plaintiff would not have entrusted her PII and PHI to Defendants had she known that Defendants failed to maintain adequate data security.

15. Plaintiff and other class members received the following letter dated December 12, 2024, stating that her information was compromised (the "Notice Letter").



ConnectOnCall

December 12, 2024

[redacted]
TIFFANY PICKLESIMER
[redacted]

NOTICE OF DATA BREACH

Dear Tiffany Picklesimer:

ConnectOnCall.com, LLC provides a product ("ConnectOnCall") that healthcare providers purchase to improve their after-hours call process and enhance communications between the providers and their patients. I am writing to inform you about an incident that involved personal information about you relating to your communications with a healthcare provider that uses ConnectOnCall. We regret that this incident occurred and take the security of personal information seriously. We are sending you this correspondence to tell you what happened, what information was involved, what we have done, and what you can do to address this situation.

WHAT HAPPENED. On May 12, 2024, we learned of an issue impacting ConnectOnCall. As soon as we learned of the incident, we immediately began an investigation and took steps to secure the product and ensure the overall security of our environment. Our investigation revealed that between February 16, 2024, and May 12, 2024, an unknown third party had access to ConnectOnCall and certain data within the application, including certain information in provider-patient communications.

WHAT INFORMATION WAS INVOLVED. You are receiving this notice because you or your family member, health advocate, or healthcare provider provided your information in a patient-provider message using ConnectOnCall. We have determined that the personal information involved in this incident may have included your name, phone number, and information related to your health conditions, treatments, or prescriptions.

WHAT WE ARE DOING. We engaged external cybersecurity specialists to determine the full nature and scope of the incident, identify any impacted information, and help us enhance our security controls to mitigate the risk of future security incidents. Also, after becoming aware of the incident, we took the ConnectOnCall product offline and have been working through a phased restoration of the product in a new, more secure environment. We also notified federal law enforcement of the incident.

WHAT YOU CAN DO. Consistent with certain laws, we are providing you with the following information about steps that a consumer can take to protect against potential misuse of personal information.

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.ftc.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

16. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect herself from data breaches, and reviewing her financial accounts for fraud or suspicious activity. She now plans to spend several hours a month checking account statements for irregularities.

17. As a result of the Data Breach and the release of her PHI and PII, which she expected Defendants to protect from disclosure, Plaintiff has suffered emotional distress, including

anxiety, concern, and unease about unauthorized parties viewing and potentially using her PHI and PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

B. Defendants

18. Defendant Phreesia, Inc., is a Delaware corporation with its principal place of business located at 1521 Concord Pike, Suite 301, Wilmington, DE 19803.

19. Defendant ConnectOnCall, LLC is a New York limited liability company with a principal place of business located at 200 Motor Parkway, Hauppauge, New York.

20. Defendant ConnectOnCall is a wholly owned subsidiary of Defendant Phreesia. Defendant Phreesia acquired Defendant ConnectOnCall on October 3, 2023.[12] On information and belief, Defendant Phreesia is the sole member of Defendant ConnectOnCall.

IV. FACTUAL BACKGROUND

A. Defendants failed to adequately protect customer data, resulting in the Data Breach.

21. Defendants offer software to healthcare organizations and providers, focused on streamlining and supporting the administrative aspects of healthcare, including patient intake and communications. In providing such services, Defendants require Plaintiff to provide highly sensitive Personally Identifiable Information ("PII") and Protected Health Information ("PHI"). Defendant ConnectOnCall assists providers and patients in after-hours communications. After Defendant Phreesia acquired ConnectOnCall in October 2023, Defendants started offering ConnectOnCall's after-hours communication product under the name "PhreesiaOnCall" to customers.[13]

22. When patients use PhreesiaOnCall, "Phreesia's bidirectional EHR [Electronic Health Record] integration matches the caller to the correct patient, allowing the provider to review a **snapshot of the patient's history** before returning the call."[14]

---

[12] *Phreesia Announces Third Quarter Fiscal 2024 Results, supra,* note 10.

[13] *After Hours*, Phreesia, https://www.phreesia.com/after-hours/ (last visited Jan. 15, 2025).

[14] *Id.*

23. Further, Phreesia offers services assisting the patient check-in process[15] and health screening questionnaires.[16] To use these services, Plaintiff and Class Members must enter their private information into a check-in form[17] or questionnaire[18] to receive medical and/or health related services.

24. According to Phreesia's Platform Privacy Policy, Defendants collect "personal data about your health" which "may include the health information you entered into your Healthcare Provider's intake forms on the Phreesia platform, as well as information that your Healthcare Provider has gathered and included in your medical, insurance or appointment records."[19] Further, Defendants collect "[i]nformation you voluntarily enter into the screens (for example, if you answer survey questions or provide contact information for follow-up from a third party); [i]nformation about the health-related materials you see; and … device and network information, log files and analytics information … IP addresses, browser type, date/time stamp, and number of clicks."[20]

25. Defendants' claim: "Privacy and security are top priorities to us-not boxes to be checked during a once-a-year review. At every level of our organization, we have measures and protocols in place to protect your information, and we foster a culture focused on safeguarding data. We're honored to have those efforts recognized with many of the industry's most well-known certifications."[21]

26. Notwithstanding these promises, an investigation revealed that ConnectOnCall experienced a data breach between February 16, 2024 and May 12, 2024 affecting up to 914,138

[15] *Registration*, Phreesia, https://www.phreesia.com/products/registration/ (last visited Jan. 6, 2025).

[16] *Collect Patient-Reported Data*, Phreesia, https://www.phreesia.com/products/collect-patient-reported-data/ (last visited Jan. 6, 2025).

[17] *Registration, supra*, note 16.

[18] *Collect Patient-Reported Data*, *supra* note 17.

[19] *Privacy Policy*, Phreesia, https://www.phreesia.com/privacy-policy/ (last visited Jan. 6, 2025).

[20] *Id.*

[21] *Id.*

people.[22] Personal information involved in this data breach include "information shared in communications between patients and their healthcare providers such as names and phone numbers, and may have also included medical record numbers, dates of birth, and information related to health conditions, treatments, or prescriptions...."[23] Further, "Social Security Numbers may have also been impacted."[24]

27. As a condition of providing services, Defendants receive, create, and handle the PII and PHI of Plaintiff and Class Members.

28. Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep it confidential.

29. Due to the sensitivity of the PII and PHI that Defendants handle, Defendants are aware of their critical responsibility to safeguard this information—and, therefore, how devastating its theft is to individuals whose information has been stolen.

30. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, Defendants assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

31. Despite the existence of these duties, Defendants failed to implement reasonable data security measures to protect the information with which it was entrusted, and ultimately allowed nefarious third-party hackers to compromise Plaintiff's and Class Members' PII and PHI.

B. Defendants were well aware of the need to take special care with consumers' PII, PHI and medical information.

32. Defendants claim to maintain protected information in compliance with HIPAA requirements.[25]

---

[22] *ConnectOnCall Announces 914K-Record Data Breach*, *supra* note 8.

[23] *ConnectOnCall.com LLC Provide Notice of Data Security Incident*, Business Wire, https://www.businesswire.com/news/home/20241211221827/en/ConnectOnCall.com-LLC-Provides-Notice-of-Data-Security-Incident (last visited Jan. 2, 2025).

[24] *Id.*

[25] *Privacy Policy*, *supra* note 20.

33. Defendants made these representations concerning securing consumers' PII and PHI because they knew and understood the severe consequences of losing this data.

34. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (Personal Information)" so that these companies can take the necessary precautions to thwart such attacks.[26]

35. The healthcare industry has become a rich target for hackers: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[27] "The IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific—and now obsolete—operating systems and cannot be transferred to supported operating systems."[28]

36. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[29] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

---

[26] Reuters, FBI warns healthcare firms they are targeted by hackers, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Jan. 6, 2025).

[27] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Jan. 6, 2025).

[28] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names.

[29] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited Jan. 6, 2025).

C. Defendants failed to comply with regulatory guidance and industry-standard cybersecurity practices.

37. Defendants' data security failure stems from their failure to comply with state and federal laws and requirements as well as industry standards governing the protection of PII and PHI.

38. At least 24 states have enacted laws addressing data security practices that require businesses that own, license or maintain PII to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access.

39. Defendants also failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendants. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

40. The FTC recommends:

- limiting access to customer information to employees who have a business reason to see it;
- keeping customer information in encrypted files provides better protection in case of theft;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;
- using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
- monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and,
- monitoring activity logs for signs of unauthorized access to customer information.[30]

[30] Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last visited June 13, 2024).

41. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

42. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[32] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

43. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

44. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

---

[31] Federal Trade Commission, *Start With Security* at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 6, 2025).

[32] Federal Trade Commission, *Protecting PII: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited June 13, 2024).

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

47. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[33] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[34]

48. On October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[35] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[36]

49. Defendants were aware of their obligations to protect customers' PII, PHI and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers from unauthorized access. In this case, Defendants were at all times fully aware of obligation to protect the PII and PHI of Defendants' customers because of their status as one of the largest pharmaceutical distribution managers in the nation. Defendants were also aware of the significant repercussions if they failed to do so because Defendants collected PII and PHI from millions of

[33] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Jan. 6, 2025).

[34] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited June 13, 2024).

[35] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited Jan. 15, 2025).

[36] *Id.*

consumers and knew that this PII and PHI, if hacked, would result in injury to consumers, including Plaintiff and Class Members.

50. Based upon the known details of the Data Breach and how it occurred, Defendants also failed to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, and intrusion detection and prevention.

D. Defendants failed to comply with HIPAA's data security requirements.

51. Defendants are covered by HIPAA (see 45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule.[37] These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

52. HIPAA prohibits unauthorized disclosures of "protected health information" and it requires that Defendants implement appropriate safeguards for this information. HIPAA requires that entities covered by its rules, including Defendants, provide notice of a breach of unsecured protected health information—i.e., non-encrypted data—without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

53. Following a data breach at a HIPAA covered entity, the HIPAA Omnibus Rule dictates it "must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported." The four-factor risk assessment includes:

a) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers);

b) the recipient of the PHI;

[37] 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

c) whether the PHI was actually acquired or viewed; and,

d) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[38]

54. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information.

55. Defendants failed to comply with these HIPAA requirements and, indeed, their own Privacy Practices. Defendants did not:

a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b) Adequately protect Plaintiff's and the Class Members' Personal Information;

c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding

[38] 78 Fed. Reg. 5641-46; *see also* 45 C.F.R. § 164.304.

individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h) Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

i) Conduct the four-factor Risk Analysis following the Data Breach;

j) Properly send timely notice to Plaintiff and the Classes pursuant to 45 C.F.R. §§ 164.400-414;

k) Ensure compliance with the electronically protected health information security standard rules by their workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

l) Train all members of their workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. §164.530(b).

E. The Data Breach puts Plaintiff and Class Members at increased risk of fraud and identity theft.

56. Defendants' failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII and PHI stolen in the Data Breach—names, addresses, zip codes, phone numbers, email addresses, dates of birth, Social Security Numbers, and health insurance account information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. As a result, Plaintiff and Class Members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

57. There is little doubt that consumers' PII and PHI from the Data Breach will be circulating on the dark web, as it is highly valuable. Malicious actors use PII and PHI to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII and PHI to open new financial accounts, open new utility

accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."[39]

58. Further, identity thieves often wait months or years to use PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiff's and Class Members' data may have been compromised in other data breaches, the fact that the Breach centralizes the PII and PHI and identifies the victims as Defendants' customers materially increases the risk to Plaintiff and the Class.

59. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[40] Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiff and Class Members will therefore need to spend time and money to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach. In other words, Plaintiff and Class Members have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Data Breach.

60. Plaintiff and Class Members have also realized harm in the lost or reduced value of their PII. Defendants admit the PII compromised in the Breach is valuable. Defendants collect, retain, and use Plaintiff's and Class Members' PII to earn revenue. Plaintiff's and Class Members'

[39] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

[40] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (2007), https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last visited Jan. 6, 2025).

PII is not only valuable to Defendants, but Plaintiff and Class Members also place value on their PII based on their understanding that their PII is a financial asset to companies who collect it.[41]

61. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's unauthorized access to Plaintiff's and Class Members' PII and PHI that was permitted without authorization by Defendants. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

62. Moreover, Plaintiff and Class Members value the privacy of this information and expect Defendants to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Defendants, provided their PII and payment card information, or paid the same prices for Defendants' goods and services had they known Defendants did not implement reasonable security measures to protect their PII.[42] Customers reasonably expect that the payments they make to Defendants and those made on their behalf through government programs and insurance, incorporate the costs to implement reasonable security measures to protect customers' PII. And because consumers value data privacy and security, companies with robust data security practices can command higher prices than those who do not. As a result, Plaintiff and Class Members did not receive the benefit of their bargain with Defendants because they paid for services they expected but did not receive.

63. Given Defendants' failure to protect their PII and PHI, Plaintiff and Class Members have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering further harm, as their PII and PHI remains in Defendants' possession. Accordingly, this action represents

---

[41] *See, e.g.*, Ponemon Institute, LLC, *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at $55.70), available at https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html.

[42] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last accessed June 13, 2024) (noting approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less PII to organizations that suffered a data breach).

the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

64. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their PII and PHI and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII and PHI; (iii) loss of value of their PII and PHI; (iv) the lost value of unauthorized access to Plaintiff's and Class Members' PII and PHI permitted by Defendants; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; (vi) Defendants' retention of profits attributable to Plaintiff's and Class Members' PII and PHI that Defendants failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to Defendants for goods and services purchased, as Plaintiff and Class Members reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII and PHI, which was not the case; and (x) nominal damages.

V. CLASS ACTION ALLEGATIONS

65. Plaintiff brings this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed Nationwide Class defined as:

> All natural persons in the United States whose Personally Identifiable Information and/or Protected Health Information was compromised as a result of the Data Breach.

66. In addition, the Florida Subclass is defined as follows:

> **Florida Subclass**: All natural persons in the State of Florida whose Personally Identifiable Information and/or Protected Health Information was compromised as a result of the Data Breach.

67. The Nationwide Class and Florida Subclass are collectively referred to herein as the "Class."

68. **Numerosity and Ascertainability:** Plaintiff does not know the exact size of the Class or identity of the Class members, since such information is in the exclusive control of Defendants. Nevertheless, the Class encompasses at least hundreds of thousands of individuals

dispersed throughout the United States. The number of Class members is so numerous that joinder of all Class members is impracticable. The names, addresses, and phone numbers of Class members are identifiable through documents maintained by Defendants.

69. **Commonality and Predominance:** This action involves common questions of law and fact which predominate over any question solely affecting individual Class members. These common questions include:

a. whether Defendants engaged in the conduct alleged herein;

b. whether Defendants had a legal duty to use reasonable security measures to protect Plaintiff and Class members' PII and PHI;

c. whether Defendants violated HIPAA;

d. whether Defendants timely, accurately, and adequately informed Plaintiff and Class members that their PII and PHI had been compromised;

e. whether Defendants breached their legal duties by failing to protect the PII and PHI of Plaintiff and Class members;

f. whether Defendants acted reasonably in securing the PII and PHI of Plaintiff and Class members;

g. whether Plaintiff and Class members are entitled to injunctive relief; and

h. whether Plaintiff and Class members are entitled to damages and equitable relief.

70. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because all Class members were comparably injured through Defendants' substantially uniform misconduct, as described above. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other members of the Class that they represent, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and Class members arise from the same operative facts and are based on the same legal theories.

71. **Adequacy:** Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other members of the Class she seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; and Plaintiff

intends to prosecute this action vigorously. The Class's interest will be fairly and adequately protected by Plaintiff and her counsel.

72. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other detriment suffered by Plaintiff and other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be virtually impossible for the Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not: individualized litigation creates a potential for inconsistent or contradictory judgments, increases the delay and expense to the parties, and increases the expense and burden to the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by this Court.

VI. CAUSES OF ACTION

A. Claims Brought on Behalf of the Nationwide Class

COUNT ONE
NEGLIGENCE

73. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

74. Defendants owed a duty to Plaintiff and Class members, arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of their data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures, and practices to ensure that Plaintiff's and Class members' information was adequately secured from unauthorized access.

75. Defendants' Privacy Policies acknowledged Defendants' duty to adequately protect Plaintiff's and Class members' PII and PHI.

76. Defendants are covered by HIPAA (see 45 C.F.R. § 160.102) and, as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

77. Defendants owed a duty to Plaintiff and Class members to implement administrative, physical, and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and Class members' PII and PHI.

78. Defendants also had a duty to only maintain PII and PHI that was needed to serve customer needs.

79. Defendants owed a duty to disclose the material fact that their data security practices were inadequate to safeguard Plaintiff and Class members' PII and PHI.

80. Defendants also had independent duties under Plaintiff's and Class members' state laws that required Defendants to reasonably safeguard Plaintiff's and Class members' PII and PHI, and promptly notify them about the Data Breach.

81. Defendants had a special relationship with Plaintiff and Class members as a result of being entrusted with their PII and PHI, which provided an independent duty of care. Plaintiff's and Class members' willingness to entrust Defendants with their PII and PHI was predicated on the understanding that Defendants would take adequate security precautions. Moreover, Defendants were capable of protecting their networks and systems, and the PII and PHI they stored on them, from unauthorized access.

82. Defendants breached their duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiff's and Class members' PII and PHI, including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that their data security practices were inadequate to safeguard Plaintiff's and Class members' PII and PHI.

83. But for Defendants' breach of duties, including the duty to use reasonable care to protect and secure Plaintiff's and Class members' PII and PHI, Plaintiff's and Class members' PII and PHI would not have been accessed by unauthorized parties.

84. Plaintiff and Class members were foreseeable victims of Defendants' inadequate data security practices. Defendants knew or should have known that a breach of their data security systems would cause damage to Plaintiff and Class members.

85. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiff's and Class members' PII and PHI would result in unauthorized access to Defendants' networks, databases, and computers that stored or contained Plaintiff's and Class members' PII and PHI.

86. As a result of Defendants' negligent failure to prevent the Data Breach, Plaintiff and Class members suffered injury, which includes, but is not limited to, exposure to a heightened and imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class members have also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiff's and Class members' PII and PHI has also diminished the value of the PII and PHI.

87. The harm to Plaintiff and Class members was a proximate, reasonably foreseeable result of Defendants' breaches of the aforementioned duties.

88. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE

89. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

90. Under the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

91. In addition, under state data security statutes, Defendants had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class members' PII.

92. Defendants breached these duties to Plaintiff and Class members, under the FTCA and the state data security statutes, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

93. Defendants are covered by HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. HIPAA prohibits unauthorized disclosures of "protected health information." which includes the information at issue here.

94. Plaintiff and Class members were foreseeable victims of Defendants' violations of the FTCA, HIPAA and state data security statutes. Defendants knew or should have known that the failure to implement reasonable measures to protect and secure Plaintiff's and Class members' PII would cause damage to Plaintiff and Class members.

95. Defendants' failure to comply with the applicable laws and regulations constitutes negligence *per se.*

96. But for Defendants' violation of the applicable laws and regulations, Plaintiff's and Class members' PII would not have been accessed by unauthorized parties.

97. As a result of Defendants' failure to comply with applicable laws and regulations, Plaintiff and Class members suffered injury, which includes, but is not limited to, the exposure to a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class members also have incurred, and will

continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class members' PII has also diminished the value of the PII.

98. The harm to Plaintiff and the Class members was a proximate, reasonably foreseeable result of Defendants' breaches of the applicable laws and regulations.

99. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

COUNT THREE
GROSS NEGLIGENCE

100. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

101. Plaintiff and Class members entrusted Defendants with highly-sensitive and inherently personal private data subject to confidentiality laws.

102. In requiring, obtaining and storing Plaintiff's and Class members' PII and PHI, Defendants owed a duty of reasonable care in safeguarding the PII and PHI.

103. Defendants' networks, systems, protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiff's and Class members' PII and PHI were secured from unauthorized access.

104. Defendants' networks, systems, protocols, policies, procedures, and practices, as described above, were not reasonable given the sensitivity of the Plaintiff's and Class members' private data and the known vulnerabilities of Defendants' systems.

105. Defendants did not comply with state and federal laws and rules concerning the use and safekeeping of this private data.

106. Upon learning of the Data Breach, Defendants should have immediately disclosed the Data Breach to Plaintiff and Class members, credit reporting agencies, the Internal Revenue Service, financial institutions, and all other third parties with a right to know and the ability to mitigate harm to Plaintiff's and Class members as a result of the Data Breach.

107. Despite knowing their networks, systems, protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiff's and Class members' PII and PHI were secured from unauthorized access, Defendants ignored the inadequacies and were oblivious to the risk of unauthorized access they had created.

108. Defendants' behavior establishes facts evidencing a reckless disregard for Plaintiff's and Class members' rights.

109. Defendants, therefore, were grossly negligent.

110. Defendants' negligence also constitutes negligence per se.

111. The negligence is directly linked to injuries.

112. As a result of Defendants' reckless disregard for Plaintiff's and Class members' rights by failing to secure their PII and PHI, despite knowing their networks, systems, protocols, policies, procedures, and practices were not adequately designed, implemented, maintained, monitored, and tested, Plaintiff and Class members suffered injury, which includes, but is not limited to, the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class members' PII and PHI has also diminished the value of the PII and PHI.

113. The harm to Plaintiff and the Class members was a proximate, reasonably foreseeable result of Defendants' breaches of the applicable laws and regulations.

114. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

COUNT FOUR
BREACH OF IMPLIED CONTRACTS

115. Plaintiff incorporates the foregoing allegations in paragraphs as if fully set forth herein.

116. Plaintiff and Class members were required to provide their PII and PHI to obtain services from Defendants. Plaintiff and Class members entrusted their PII and PHI to Defendants in order to obtain services from them.

117. By providing their PII and PHI, and upon Defendants' acceptance of such information, Plaintiff and Class members on one hand, and Defendants on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the services provided, whereby Defendants were obligated to take reasonable steps to secure and safeguard that information.

118. Defendants had an implied duty of good faith to ensure that the PII and PHI of Plaintiff and Class members in their possession was only used in accordance with their contractual obligations.

119. Defendants were therefore required to act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiff's and Class members' PII and to comply with industry standards and state laws and regulations for the security of this information, and Defendants expressly assented to these terms in their Privacy Policies as alleged above.

120. Under these implied contracts for data security, Defendants were further obligated to provide Plaintiff and all Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and PHI.

121. Plaintiff and Class members performed all conditions, covenants, obligations, and promises owed to Defendants, including paying for the services provided by Defendants and/or providing the PII and PHI required by Defendants.

122. Defendants breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class members' PII and PHI, resulting in the Data

Breach. Defendants unreasonably interfered with the contract benefits owed to Plaintiff and Class members.

123. Further, on information and belief, Defendants have not yet provided Data Breach notifications to some affected Class members who may already be victims of identity fraud or theft, or are at imminent risk of becoming victims of identity theft or fraud, associated with the PII or PHI that they provided to Defendants. These Class members are unaware of the potential source for the compromise of their PII and PHI.

124. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

125. As a result of Defendants' conduct, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value as compared to the secure services they paid for. Plaintiff and Class members, therefore, were damaged in an amount at least equal to the difference in the value of the secure services they paid for and the services they received.

126. Neither Plaintiff, nor Class members, nor any reasonable person would have provided their PII and PHI to Defendants had Defendants disclosed that their security was inadequate or that they did not adhere to industry-standard security measures.

127. As a result of Defendants' breach, Plaintiff and Class members have suffered actual damages resulting from theft of their PII and PHI, as well as the loss of control of their PII and PHI, and remain in imminent risk of suffering additional damages in the future.

128. As a result of Defendants' breach, Plaintiff and the Class members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII and PHI. As a result, Plaintiff and the Class members have suffered actual identity theft and the ability to control their PII and PHI.

129. Accordingly, Plaintiff and Class members have been injured as a result of Defendants' breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT FIVE
UNJUST ENRICHMENT

130. Plaintiff incorporates the foregoing allegations in paragraphs as if fully set forth herein.

131. Plaintiff and Class members conferred a monetary benefit on Defendants in the form of monetary payments—directly or indirectly—for services received.

132. Defendants collected, maintained, and stored the PII and PHI of Plaintiff and Class members and, as such, Defendants had knowledge of the monetary benefits conferred by Plaintiff and Class members.

133. The money that Plaintiff and Class members paid to Defendants should have been used to pay, at least in part, for the administrative costs and implementation of data management and security. Defendants failed to implement—or adequately implement—practices, procedures, and programs to secure sensitive PII and PHI, as evidenced by the Data Breach.

134. As a result of Defendants' failure to implement security practices, procedures, and programs to secure sensitive PII and PHI, Plaintiff and Class members suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiff and Class members paid for, and the services they received without reasonable data privacy.

135. Under principles of equity and good conscience, Defendants should not be permitted to retain money belonging to Plaintiff and Class members because Defendants failed to implement the data management and security measures that are mandated by industry standards and that Plaintiff and Class members paid for.

136. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by Defendants. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendants traceable to Plaintiff and the Class.

COUNT SIX
DECLARATORY JUDGMENT

137. Plaintiff incorporates the foregoing allegations in paragraphs as if fully set forth herein.

138. Plaintiff and the Class have stated claims against Defendants based on negligence, negligence per se and gross negligence, and violations of various state and federal statutes.

139. Defendants failed to fulfill their obligations to provide adequate and reasonable security measures for the PII and PHI of Plaintiff and the Class, as evidenced by the Data Breach.

140. As a result of the Data Breach, Defendants' systems are more vulnerable to unauthorized access and require more stringent measures to be taken to safeguard the PII and PHI of Plaintiff and the Class going forward.

141. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' current obligations to provide reasonable data security measures to protect the PII and PHI of Plaintiff and the Class. Defendants maintain that their security measures were—and still are—reasonably adequate and deny that they previously had or have any obligation to implement better safeguards to protect the PII and PHI of Plaintiff and the Class.

142. Plaintiff seeks a declaration that Defendants must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII and PHI of Plaintiff and the Class. Specifically, Plaintiff and the Class seek a declaration that Defendants' existing security measures do not comply with their obligations, and that Defendants must implement and maintain reasonable security measures on behalf of Plaintiff and the Class to comply with their data security obligations.

B. Claims Brought on Behalf of Plaintiff and the Florida Subclass

COUNT SEVEN
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
F.S.A. § 501.201, et. seq.

143. Plaintiff, individually and on behalf of the Florida Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This Claim is brought individually and on behalf of the Florida Subclass under the laws of Florida.

144. Plaintiff and Florida Subclass members are "consumers" as defined by F.S.A. § 501.203(7).

145. Defendants ConnectOnCall and Phreesia advertised, offered or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

146. Defendants engaged in unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts in the conduct of trade or commerce in violation of F.S.A. § 501.204(1), including:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Florida Subclass Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d) Failing to comply with Florida's Information Protection Act ("FIPA"), F.S.A. § 501.171, et. seq., which requires entities "to take reasonable measures to protect and secure data in electronic form containing personal information."

e) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Florida Subclass Members' PII, including by implementing and maintaining reasonable security measures;

f) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII and PHI, including duties imposed by FIPA and the FTC Act, 15 U.S.C. § 45.

g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Florida Subclass Members' PII; and

h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by FIPA and the FTC Act, 15 U.S.C. § 45.

147. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

148. Had Defendants disclosed to Plaintiff and Subclass Members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Defendants were trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of their security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

149. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

150. Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

VII. PRAYER FOR RELIEF

Plaintiff, on behalf of herself and on behalf of the proposed Nationwide Class and Subclass,

requests that the Court:

a. Certify this case as a class action, appoint Plaintiff as a class representative, and appoint Plaintiff's Counsel as Class Counsel for Plaintiff to represent the Class;

b. Find that Defendants breached their duty to safeguard and protect the PII and PHI of Plaintiff and Class members that was compromised in the Data Breach;

c. Award Plaintiff and Class members appropriate relief, including actual and statutory damages, restitution, and disgorgement;

d. Award equitable, injunctive, and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: January 17, 2025

Respectfully submitted,

/s/ Jonathan D. Lindenfeld

Jonathan D. Lindenfeld
FEGAN SCOTT LLC
305 Broadway, 7th Floor
New York, NY 10007
Telephone: (332) 216-2101
Facsimile: (312) 264-0100
jonathan@feganscott.com

Elizabeth A. Fegan (*pro hac vice* forthcoming)
Megan E. Shannon (*pro hac vice* forthcoming)
FEGAN SCOTT LLC
150 S. Wacker Drive, 24th Floor
Chicago, IL 60606
Telephone: (312) 741-1019
Facsimile: (312) 264-0100
beth@feganscott.com
megan@feganscott.com

Thomas E. Loeser (*pro hac vice* forthcoming)
Vara Lyons (NY Bar No. 5464524)
Ellen Wen (*pro hac vice* forthcoming)
COTCHETT, PITRE & MCCARTHY LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272
Fax: (206) 299-4184
Email: tloeser@cpmlegal.com
Email: vlyons@cpmlegal.com
Email: ewen@cpmlegal.com

Counsel for Plaintiff and the Proposed Class